CLOUDGUARD

IS001

Information Security Policy

Policy

The board and executive leadership of CloudGuard are committed to preserving the confidentiality, integrity and availability of information and information assets that the organization generates and uses.

All business operations fall under the purview of the Information Security Management System (ISMS) within CloudGuard from all locations, excluding specific activities conducted in isolated, controlled environments for testing purposes. The ISMS covers all employees and anyone working for, or on behalf of, CloudGuard and all information, information processes and infrastructure assets belonging to CloudGuard, or entrusted to CloudGuard by third parties, excluding those involved in sandboxed operations. This supports our mission to enhance the security posture of our customers by utilizing our cloud and security operations expertise through our services offerings.

CloudGuard will:

- Ensure Confidentiality is assured; Integrity and Availability of information is maintained.
- Adhere to all current legislation related to information security.
- Conduct a comprehensive risk assessment to evaluate the potential impact of a breach in confidentiality, integrity, or accessibility of our information assets and use the assessments to inform information security procedures.
- Implement and effectively operate an Information Security Management System.
- Establish confidence in our management system by obtaining certification against the ISO 27001 standard.
- Commit to continually improve our information security management system in line with the company's agile business strategy.

The organization’s business objectives are detailed in the Information Security Policies and Objectives document.

The CEO (Chief Executive Officer) has overall accountability for the policy within CloudGuard. The CISO (Chief Information Security Officer) is responsible for maintaining the policy and communicating this to all staff members and is responsible for implementing and embedding the policy. All CloudGuard employees are responsible for following the policy and related procedures. In some cases, third party organizations will be contractually required to follow aspects of the policy and related procedures.

This policy was reviewed and approved by the CloudGuard senior leadership team.

Document Control

Version	Author	Description	Approval	Date
0.1	CISO	Initial draft	CEO	22/05/2023
1.0		Approved release	CEO	22/05/2023
1.1	CISO	Removed named users, added Job titles	CEO	19/09/2023
1.2	CISO	Updated the policy statement	CEO	17/01/2024
	CISO	Annual review, no changes	CEO	15/01/2025